Near Real-time Risk Management

Transforming the Certification and Accreditation Process

Security Automation Conference

September 24, 2008

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

Agenda

- Introduction
- The Fundamentals
- The Process
- Summary

Introduction

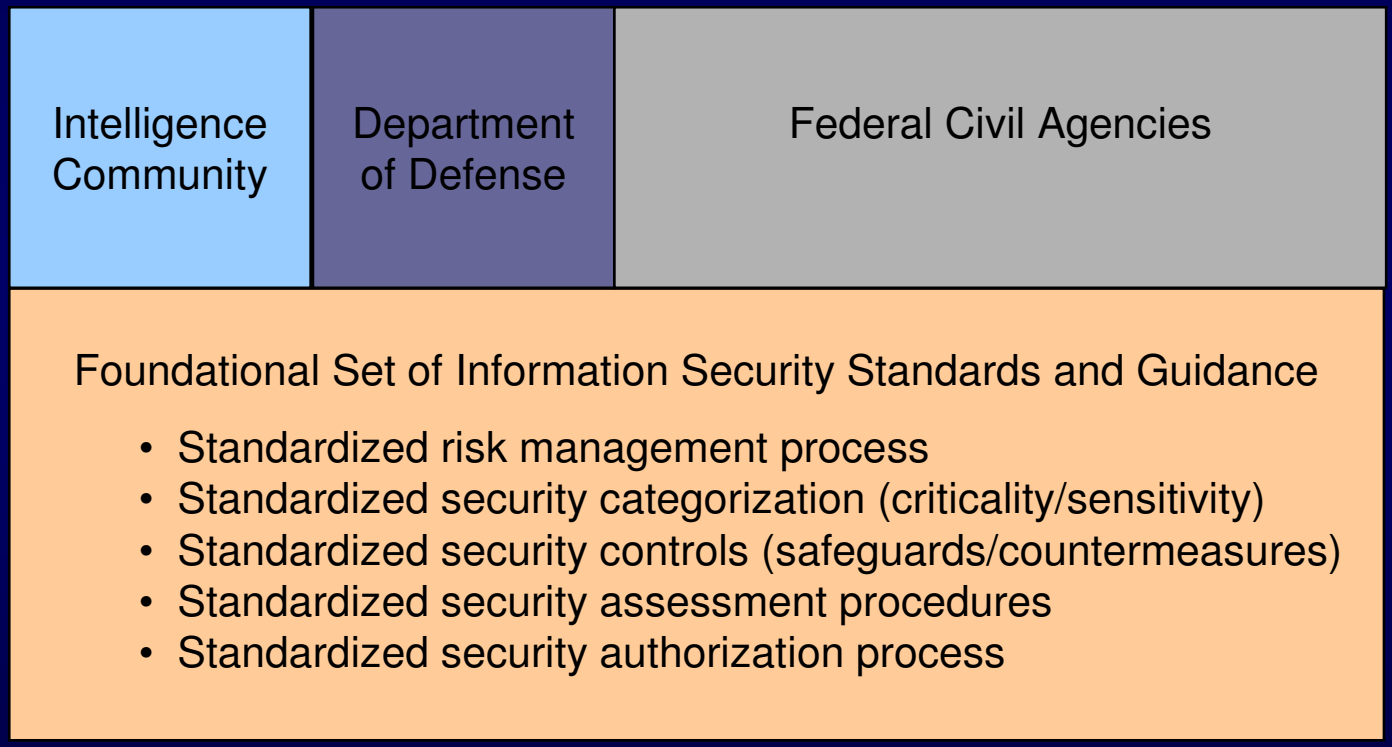
Unified Information Security Framework

The Generalized Model

Unique Information Security Requirements

The "Delta"

Common Information Security Requirements



National security and non national security information systems

Common Security Authorization Process

- NIST Special Publication 800-37, Revision 1

  Guide for Security Authorization of Federal Information Systems: A Security Life Cycle Approach

- Developed by Joint Task Force Transformation Initiative Working Group
  - *Office of the Director of National Intelligence*
  - *Department of Defense*
  - *Committee on National Security Systems*
  - *National Institute of Standards and Technology*
- Initial Public Draft (August 2008)

Purpose

Special Publication 800-37, Revision 1

- Provide guidelines for the security authorization of federal information systems to help achieve more secure systems within the federal government by:
  - Ensuring authorizing officials are appropriately engaged throughout the risk management process.
  - Promoting a better understanding of organizational risks resulting from the operation and use of information systems.
  - Supporting consistent, informed security authorization decisions.

Applicability

Special Publication 800-37, Revision 1

- Federal information systems designated as other than national security systems.
- Federal information systems designated as national security systems (U.S.C., Section 3542) as agreed upon by the Director of National Intelligence, Secretary of Defense, and Chairman, Committee on National Security Systems with augmentation and tailoring as needed to meet organizational requirements.

Applicability

Special Publication 800-37, Revision 1

- State, local, and tribal governments, as well as private sector organizations that compose the United States critical infrastructure, are encouraged to consider use of the guidelines on a voluntary basis, as appropriate.

Target Audience

Special Publication 800-37, Revision 1

- Individuals with information system development and integration responsibilities.
- Individuals with information system and security management and oversight responsibilities.
- Individuals with information system and security control assessment and monitoring responsibilities.
- Individuals with information security implementation and operational responsibilities.

Transformation Objectives

- Develop a common *security authorization process* for *all* federal information systems to ensure appropriate entities are assigned *responsibility* and are *accountable* for managing information system-related security risks.
- Express security authorization process as an integral part of the *System Development Life* Cycle and *Risk Management Framework*.

Transformation Objectives

- Incorporate a *risk executive (function)* into the security authorization process to help ensure that managing security risks from individual information systems:
  - is consistent across the organization;
  - reflects organizational risk tolerance; and
  - is performed as part of an organization-wide process that considers other organizational risks affecting mission and business success.

The Fundamentals

Main Streaming Information Security

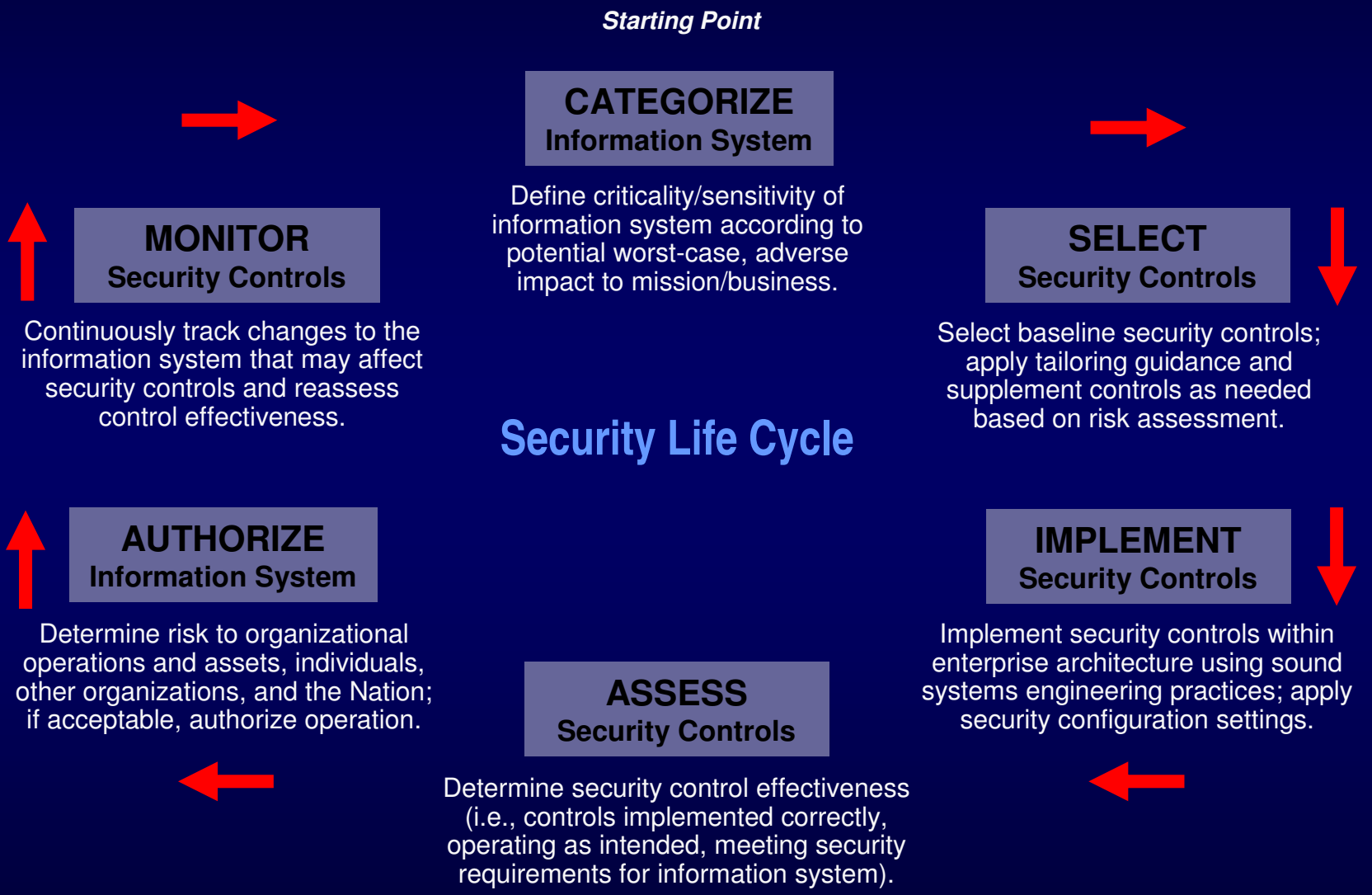
- Information security requirements must be considered *first order requirements* and are critical to mission and business success.
- An effective organization-wide information security program helps to ensure that security considerations are specifically addressed in the *enterprise architecture* for the organization and are integrated early into the *system development life cycle*.

System Development Life Cycle

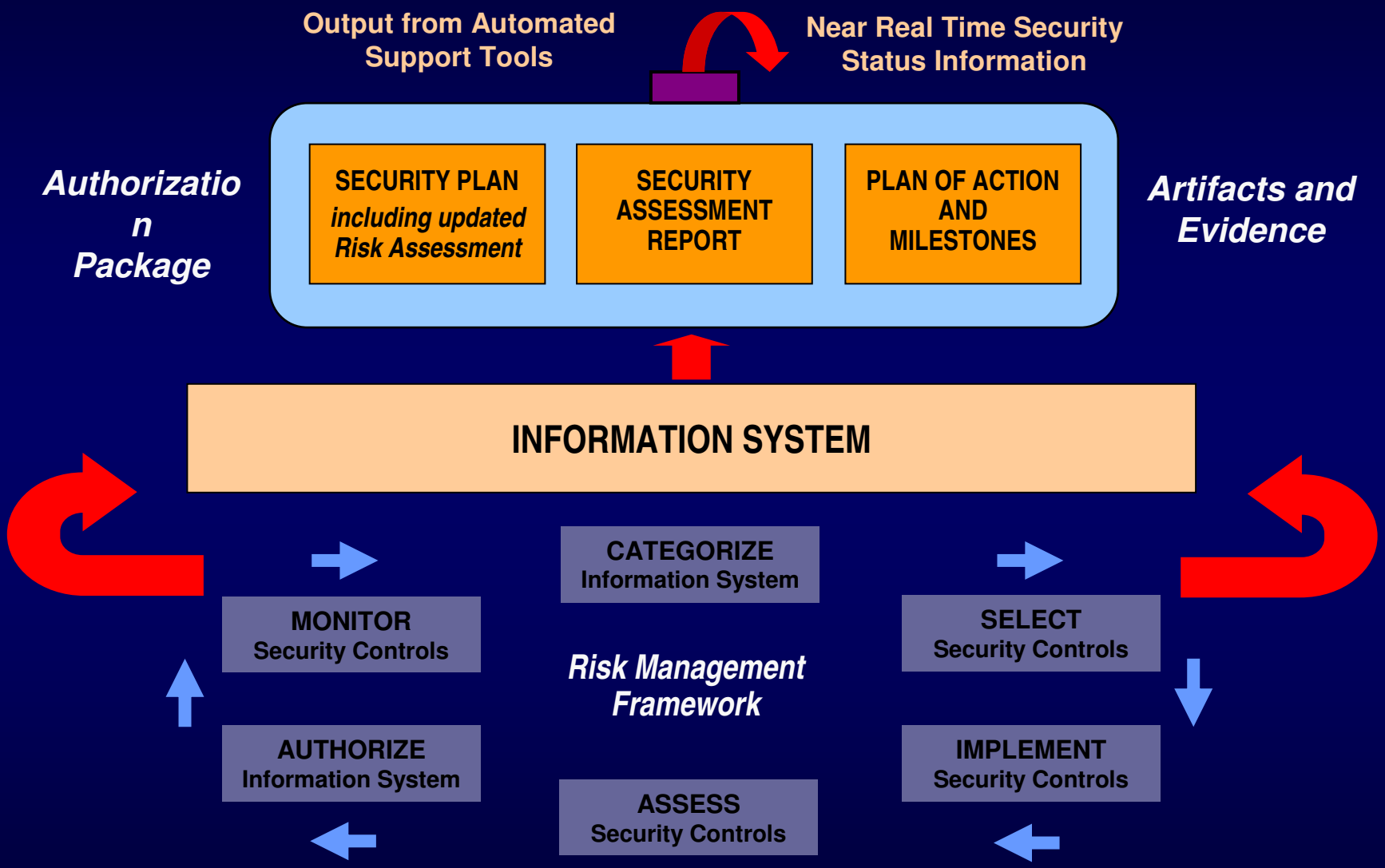
- System Initiation Phase
- System Development / Acquisition Phase
- System Implementation Phase
- System Operations / Maintenance Phase
- System Disposal Phase

Integrating security requirements into the SDLC is the most efficient and cost-effective method for an organization to ensure that its protection strategy is achieved and that authorization activities are not isolated or decoupled from the management processes employed by the organization to develop, implement, operate, and maintain information systems supporting ongoing missions or business functions…

Risk Management Framework



Applying the Risk Management Framework to Information Systems



Security Authorization Roles

- Authorizing Official
- Authorizing Official Designated Representative
- Chief Information Officer
- Senior Agency Information Security Officer
- Risk Executive (Function)
- Information System Owner

Security Authorization Roles

- Common Control Provider
- Information Owner/Steward
- Information System Security Officer
- Information System Security Engineer
- Security Control Assessor
- User Representatives

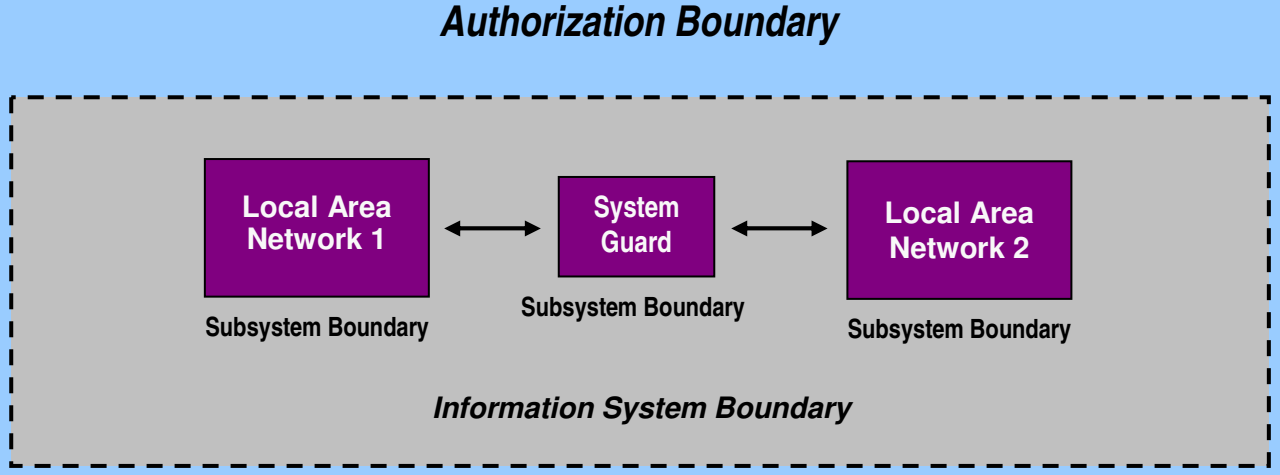
Authorization Boundaries

- Define the scope of protection for information systems (i.e., what the organization agrees to protect under its direct control or within the scope of its responsibilities).
- Include the people, processes, and technologies that are part of the systems supporting the organization's missions and business processes.
- Need to be established before information system security categorization and the development of security plans.

Authorization Boundaries

- Generally information system resources that are under the same direct management control (e.g., budgetary, programmatic, or operational authority and associated *responsibility* and *accountability*).
- May also be helpful to consider if the information resources being identified as an information system:
  - Have the same function or mission objective and essentially the same operating characteristics and information security needs; and
  - Reside in the same general operating environment (or in the case of a distributed information system, reside in various locations with similar operating environments).

Large and Complex Systems



- Security plan reflects information system decomposition with security controls assigned to each subsystem component.
- Security assessment procedures tailored for the security controls in each subsystem component and for the combined system level.
- Security control assessment performed on each subsystem component and on system-level controls not covered by subsystem security control assessments.
- Security authorization conducted on the information system as a whole.

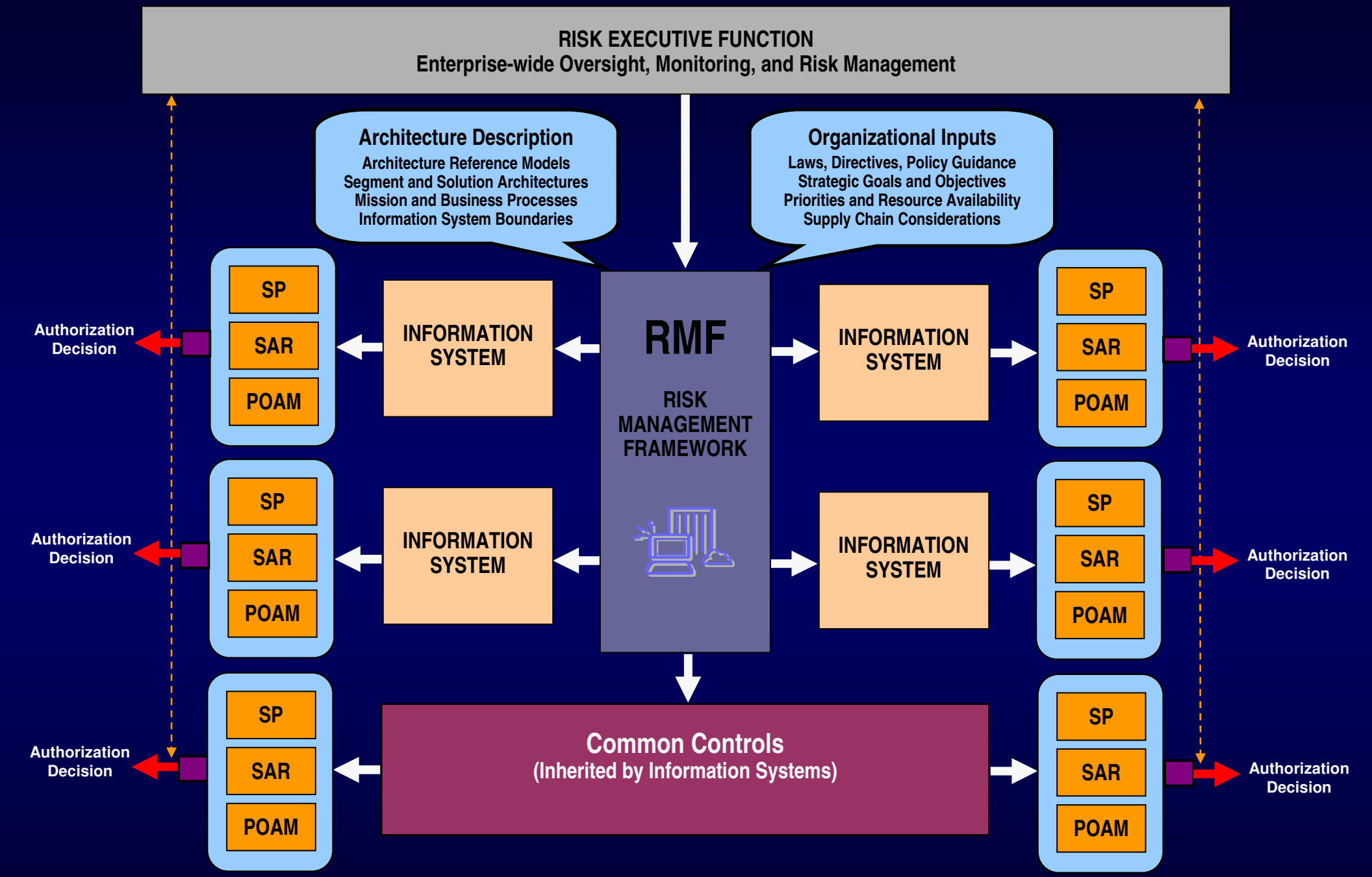
Security Control Inheritance

- Authorizing officials and information system owners are becoming increasingly dependent on security controls provided by organizational entities that are outside of their authorization boundaries, for example:
  - Organizational networks;
  - Facilities management office;
  - Human resources office;
  - Shared/external service providers.
- These security controls, often referred to as *common controls*, are typically not under the direct control of the information system owners and authorizing officials whose systems *inherit* those controls.

Security Control Inheritance

- Common controls provided by an information system owner are documented in a security plan.
- Common controls provided by entities other than information system owners are documented in a security plan or equivalent document.

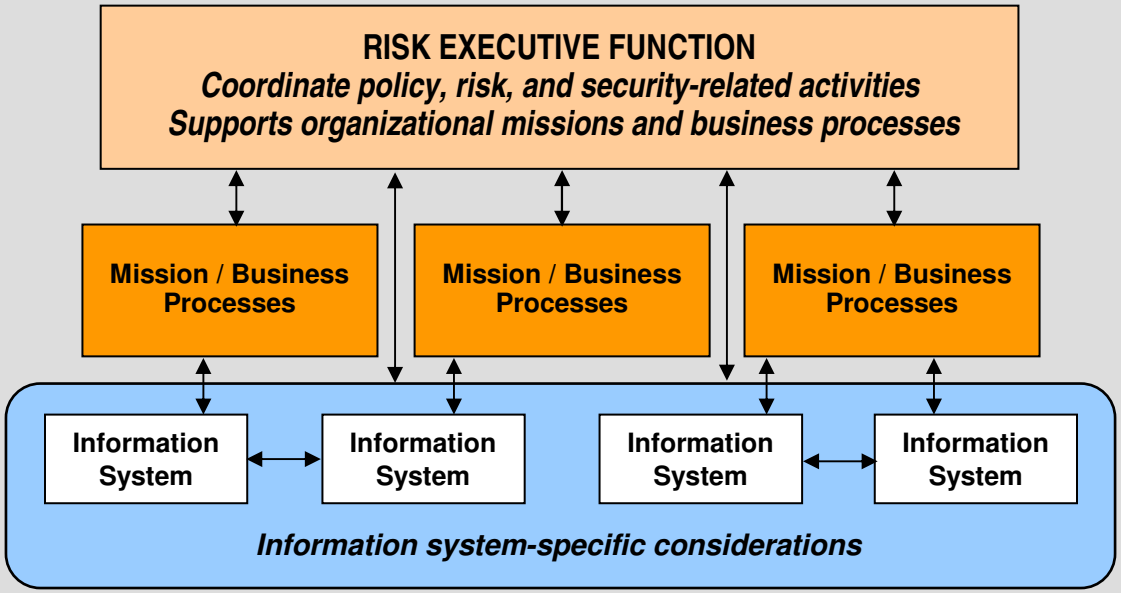
Bottom line: Every security control within an organization has an entity assigned responsibility for development, implementation, assessment for effectiveness, and authorization/approval.



NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

SP: Security Plan
SAR: Security Assessment Report
POAM: Plan of Action and Milestones

Risk Executive Function



- Establish organizational information security priorities.
- Allocate information security resources across the organization.
- Provide oversight of information system security categorizations.
- Identify and assign responsibility for common security controls.
- Provide guidance on security control selection (tailoring and supplementation).
- Define common security control inheritance relationships for information systems.
- Establish and apply mandatory security configuration settings.
- Identify and correct systemic weaknesses and deficiencies in information systems.

Security Authorization Package

- Security Plan
  - *Provides an overview of the security requirements and describes the security controls in place or planned for meeting those requirements.*
- Security Assessment Report
  - *Provides the results of assessing the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the specified security requirements.*
- Plan of Action and Milestones
  - *Describes the specific measures that are planned: (i) to correct weaknesses or deficiencies noted in the security controls during the security control assessment; and (ii) to address known vulnerabilities in the information system.*

Security Authorization Decisions

- Authorization to Operate
  - *Based on a review of the information system authorization package, the authorizing official deems the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.*
- Denial of Authorization to Operate
  - *Based on a review of the information system authorization package, the authorizing official deems the risk to organizational operations and assets, individuals, other organizations, and the Nation is unacceptable.*

Authorization Decision Document

- Authorization Decision
  - *Provides an authorization to operate or denial of authorization to operate.*
- Terms and Conditions for the Authorization
  - *Provides a description of any limitations or restrictions placed on the operation of the information system that must be followed by the system owner.*
- Authorization Termination Date
  - *Indicates when the security authorization expires and reauthorization is required.*

Reauthorization Actions

- Time Driven
  - *Reauthorization occurs when authorization termination date is reached.*
  - *Maximum authorization periods are determined by federal and organizational policies.*
- Event Driven
  - *Reauthorization occurs when there is significant change to the information system or its environment of operation.*
  - *Routine changes to an information system or its environment of operation can be handled by the organization's continuous monitoring program.*
  - *Change in authorizing official may trigger a reauthorization; but not automatically.*

Operational Scenarios

- Security authorization requirements apply only to federal information systems.
- There are two distinct types of operational scenarios that affect how organizations address security authorizations:
  - *Scenario 1: Information systems used/operated by federal agencies and their subordinate organizations; and*
  - *Scenario 2: Information systems used/operated by other organizations on behalf of federal agencies and their subordinate organizations.*

Operational Scenario One

- Information systems used or operated by a federal agency or one of its subordinate organizations:
  - *Security authorization boundary is defined by the agency or the appropriate subordinate organization of the agency;*
  - *Agency or its appropriate subordinate organization conducts all steps in the RMF to include issuing the authorization decision;*
  - *Agency or its appropriate subordinate organization maintains complete control over the security controls employed within the information system to protect organizational missions and business functions.*

Operational Scenario Two

- Information systems used or operated by *another organization* on behalf of a federal agency or one of its subordinate organizations:

  Case A: Organization contracted to federal agency or one of its subordinate organizations—

  - *Security authorization boundary is defined by the agency or its appropriate subordinate organization in consultation with the organization;*
  - *Contractor can conduct all security authorization tasks except those tasks which must be carried out by the federal agency or its appropriate subordinate organization as part of the agency's inherent governmental responsibilities.*
  - *Contractor provides appropriate evidence in the security authorization package for the authorization decision by the federal agency or its appropriate subordinate organization;*
  - *Agency or its appropriate subordinate organization provides authorization-related inputs to the contractor, as needed, and maintains oversight on all contractor-executed steps in the RMF.*

Operational Scenario Two

- Information systems used or operated by *another organization* on behalf of a federal agency or one of its subordinate organizations:

  Case B: Organization is a federal agency or one of its subordinate organizations—

  - *Security authorization boundary is defined by the agency or its appropriate subordinate organization in consultation with the organization;*
  - *Organization can conduct all steps in the RMF to include the information system authorization step and authorization decision;*
  - *Security authorization decision can also be a joint authorization decision if both parties agree to share the authorization responsibilities.*
  - *In situations where a federal agency or one of its subordinate organizations uses or operates an information system on behalf of multiple federal agencies or their subordinate organizations, the joint authorization can include all participating agencies and organizations.*

Continuous Monitoring

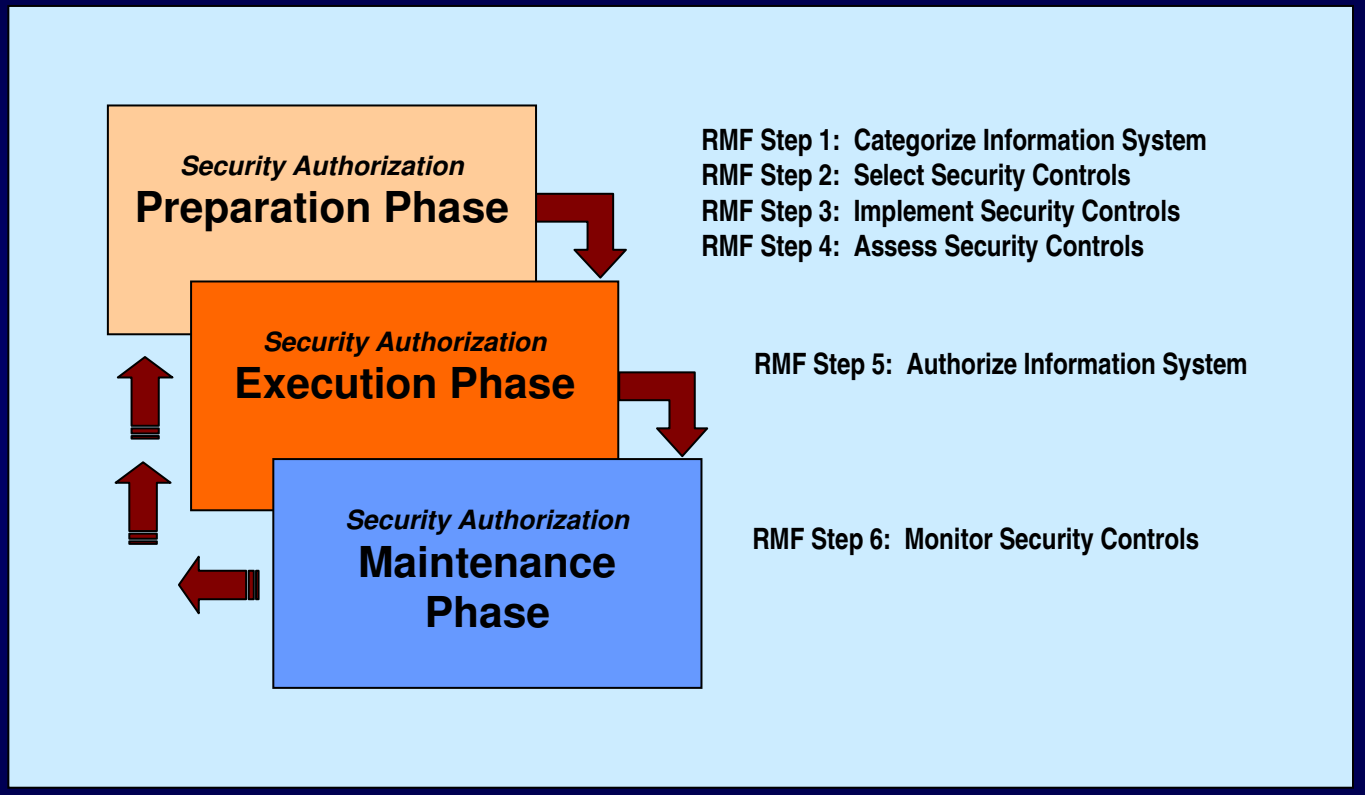
- Continuous monitoring programs determine if the security controls in information systems continue to be effective over time in light of the inevitable changes that occur in the systems as well as the environments in which the systems operate.
- Continuous monitoring programs create dynamic processes that provide essential, near real-time security status-related information to organizational officials in order to take needed risk mitigation actions and make credible, risk-based decisions regarding the operation of the information system.
- Continuous monitoring programs are most effective when supported by automated tools.

Continuous Monitoring Programs

- An effective continuous monitoring program includes:
  - *Configuration management and control processes for information systems;*
  - *Security impact analyses on actual or proposed changes to information systems and environments of operation;*
  - *Assessment of selected security controls based on continuous monitoring strategy;*
  - *Security status reporting to appropriate organizational officials;*
  - *Active involvement by authorizing officials in the ongoing management of information system-related security risks.*

The Process

Security Authorization Process



Authorization Task Structure

- Task Section
  - *Describes the specific security authorization task within the appropriate security authorization phase and step in the Risk Management Framework.*
- Primary Responsibility Section
  - *Lists the individual or group within the organization having primary responsibility for executing the security authorization task.*
- Supporting Roles Section
  - *Lists the supporting roles within the organization that may be necessary to help the individual or group with primary responsibility for executing the security authorization task.*
- SDLC Phase Section
  - *Lists the particular phase of the SDLC when the security authorization task is typically executed.*

Authorization Task Structure

- Guidance Section
  - *Provides supplemental guidance for executing the security authorization task including additional information from relevant supporting security policies, instructions, standards, and guidelines.*
- References Section
  - *Provides general references to NIST security standards and guidelines that should be consulted for additional information with regard to executing the security authorization task.*
- NSS References
  - *Provides specific national security system references to CNSS policies and instructions that should be consulted for additional information with regard to executing the security authorization task when the general references are either insufficient or inappropriate for national security application.*

Authorization Tasks

Preparation Phase

RMF Step 1: Categorize Information System

- **SYSTEM DESCRIPTION**
  - *Task 1: Describe the information system (including system boundary) and document the description in the security plan.*
- **SYSTEM REGISTRATION**
  - *Task 2: Register the information system with appropriate organizational program/management offices.*
- **SECURITY CATEGORIZATION**
  - *Task 3: Determine the security category for the information system and document the category in the security plan.*

Authorization Tasks

Preparation Phase

RMF Step 2: Select Security Controls

- **COMMON CONTROL IDENTIFICATION**
  - *Task 1a: Identify the common controls inherited by information systems within the organization and document the controls in a security plan (or equivalent document).*
- **SECURITY CONTROL SELECTION**
  - *Task 1b: Select the security controls for the information system and document the controls in the security plan.*
- **SECURITY PLAN APPROVAL**
  - *Task 2: Review and approve the security plan.*

Authorization Tasks

Preparation Phase

RMF Step 3: Implement Security Controls

- **SECURITY CONTROL IMPLEMENTATION**
  - *Task 1: Implement the security controls specified in the security plan.*
- **SECURITY CONTROL DOCUMENTATION**
  - *Task 2: Document the security control implementation, as appropriate, in the security plan, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs).*

Authorization Tasks

Preparation Phase

RMF Step 4: Assess Security Controls

- **ASSESSOR SELECTION AND INDEPENDENCE**
  - *Task 1: Identify and select the security control assessor(s) and determine if the selected assessor(s) possess the required degree of independence for the assessment.*
- **SECURITY ASSESSMENT PLAN**
  - *Task 2: Develop a plan to assess the security controls.*
- **SECURITY ASSESSMENT PLAN APPROVAL**
  - *Task 3: Review and approve the plan to assess the security controls.*

Authorization Tasks

Preparation Phase

RMF Step 4: Assess Security Controls

- **SUPPORTING MATERIALS**
  - *Task 4: Obtain appropriate documentation, records, artifacts, test results, and other materials needed to assess the security controls.*
- **SECURITY CONTROL ASSESSMENT**
  - *Task 5: Assess the security controls in accordance with the assessment procedures defined in the security assessment plan.*
- **PRELIMINARY SECURITY ASSESSMENT REPORT**
  - *Task 6: Prepare the preliminary security assessment report documenting the issues, findings, and recommendations from the security control assessment.*

Authorization Tasks

Preparation Phase

RMF Step 4: Assess Security Controls

- **SECURITY ASSESSMENT REPORT REVIEW**
  - *Task 7: Review the preliminary security assessment report.*
- **REMEDIATION ACTIONS**
  - *Task 8: If necessary, conduct remediation actions based on the preliminary security assessment report.*
- **REMEDIATION ASSESSMENT**
  - *Task 9: Assess the remediated security controls.*

Authorization Tasks

Preparation Phase

RMF Step 4: Assess Security Controls

- **FINAL SECURITY ASSESSMENT REPORT**
  - *Task 10: Update the security assessment report and prepare the executive summary.*
- **SECURITY ASSESSMENT REPORT ADDENDUM**
  - *Task 11: If necessary, prepare an addendum to the security assessment report that reflects the initial results of the remediation actions taken and provides the information system owner or common control provider perspective on the assessment findings and recommendations.*

Authorization Tasks

Preparation Phase

RMF Step 4: Assess Security Controls

- **SECURITY PLAN UPDATE**
  - *Task 12: Update the security plan based on the findings and recommendations of the security assessment report and any remediation actions taken.*
- **PLAN OF ACTIONS AND MILESTONES**
  - *Task 13: Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report.*

Authorization Tasks

Execution Phase

RMF Step 5: Authorize Information System

- **SECURITY AUTHORIZATION PACKAGE**
  - *Task 1: Assemble the authorization package and submit to authorizing official for approval.*
- **RISK DETERMINATION**
  - *Task 2: Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.*

Authorization Tasks

Execution Phase

RMF Step 5: Authorize Information System

- **RISK ACCEPTABILITY**
  - *Task 3: Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable.*
- **SECURITY AUTHORIZATION DECISION**
  - *Task 4: Prepare the security authorization decision document and transmit authorization decision and authorization package to the information system owner.*

Authorization Tasks

Maintenance Phase

RMF Step 6: Monitor Security Controls

- **SECURITY CONTROL MONITORING STRATEGY**
  - *Task 1: Develop a strategy for the continuous monitoring of security control effectiveness and any proposed/actual changes in the information system or its environment of operation.*
- **SYSYEM AND ENVIRONMENT CHANGES**
  - *Task 2: Document the proposed or actual changes to the information system or the environment of operation.*

Authorization Tasks

Maintenance Phase

RMF Step 6: Monitor Security Controls

- **SECURITY IMPACT ANALYSIS**
  - *Task 3: Determine the security impact of the proposed or actual changes to the information system or the environment of operation in accordance with the security control monitoring strategy.*
- **ONGOING SECURITY CONTROL ASSESSMENTS**
  - *Task 4: Assess a selected subset of the security controls in the information system or the environment of operation (including those controls affected by changes to the system/environment) in accordance with the continuous monitoring strategy.*

Authorization Tasks

Maintenance Phase

RMF Step 6: Monitor Security Controls

- **ONGOING REMEDIATION ACTIONS**
  - *Task 5: Conduct remediation actions based on the results of the selected security control assessments and outstanding items in the plan of action and milestones.*
- **CRITICAL DOCUMENT UPDATES**
  - *Task 6: Update the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process.*
- **SECURITY STATUS REPORTING**
  - *Task 7: Report the security status of the information system to the authorizing official and other appropriate organizational officials on a periodic basis.*

Authorization Tasks

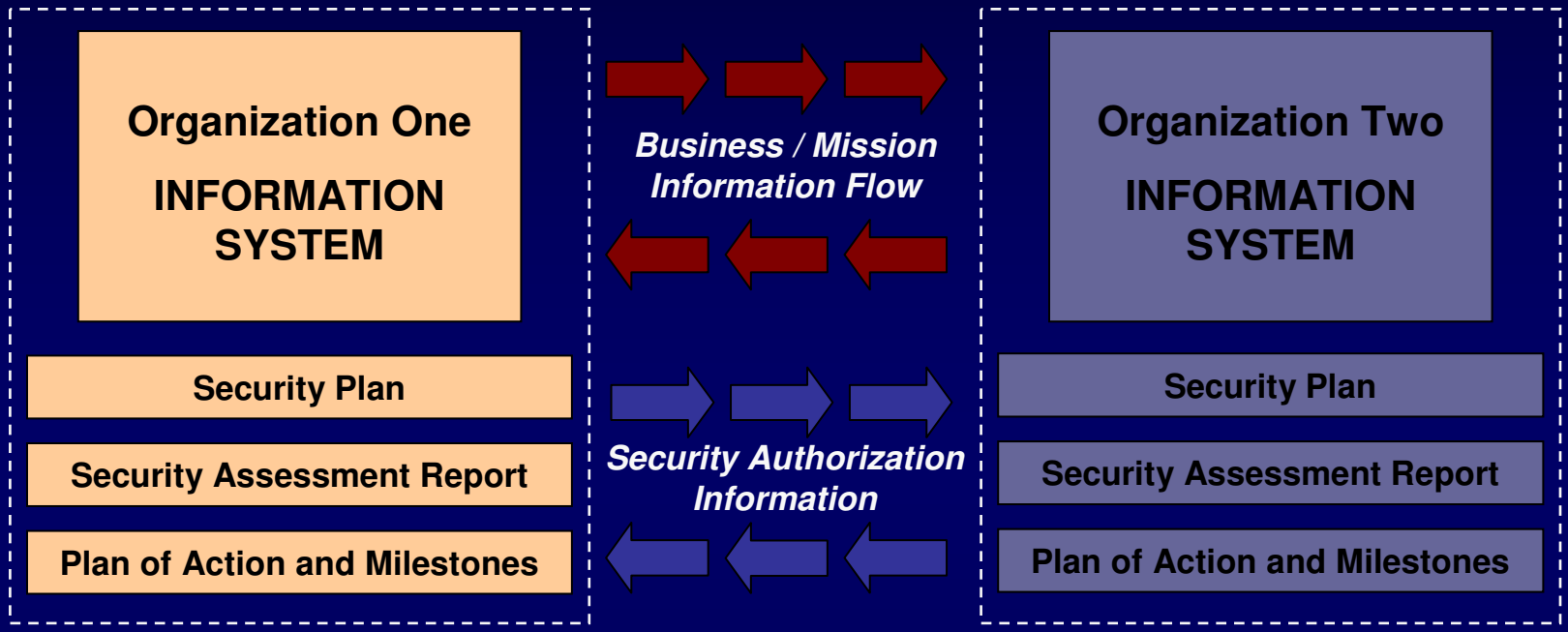
Maintenance Phase

RMF Step 6: Monitor Security Controls

- **ONGOING RISK DETERMINATION AND ACCEPTANCE**
  - *Task 8: Periodically review the reported security status of the information system and determine whether the risk to organizational operations and assets, individuals, other organizations, or the Nation remains acceptable.*
- **SYSTEM REMOVAL AND DECOMMISSIONING**
  - *Task 9: Implement an organizationally approved information system decommissioning strategy, when needed, which executes required actions when a system is removed from service.*

Summary

Recognition of Authorization Results



Determining risk to the organization's operations and assets, individuals, other organizations, and the Nation; and the acceptability of such risk.

Determining risk to the organization's operations and assets, individuals, other organizations, and the Nation; and the acceptability of such risk.

The objective is to achieve transparency of prospective partner's information security authorization processes…establishing trust relationships based on common, shared risk management principles.

Federal Risk Management Publications

- Security Categorization
  - FIPS 199 (non national security systems)
  - NIST Special Publication 800-60 (non national security systems)
  - CNSS Instruction 1199 (national security systems)
- Security Control Selection
  - FIPS 200 (non national security systems)
  - NIST Special Publication 800-53 (non national security systems)
  - CNSS Instruction 1253 (national security systems)
- Security Control Assessment
  - NIST Special Publication 800-53A (non national security systems)
  - CNSS Instruction 1253A (national security systems)
- Security Authorization
  - NIST Special Publication 800-37 (national security and non national security systems)
- Continuous Monitoring
  - NIST Special Publication 800-53A (non national security systems)
  - CNSS Instruction 1253A (national security systems)
  - NIST Special Publication 800-37 (national security and non national security systems)

Milestone Schedule

- NIST Special Publication 800-37, Revision 1

  Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach

  - Initial Public Draft: August 2008
  - Second Public Draft: December 2008
  - Final Publication: March 2009
- Download Publication from NIST Web Site

  http://csrc.nist.gov/publications/PubsDrafts.html
- Comments

  sec-cert@nist.gov

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Leader

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Administrative Support

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

Senior Information Security Researchers and Technical Support

Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

Pat Toth
(301) 975-5140
patricia.toth@nist.gov

Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Matt Scholl
(301) 975-2941
matthew.scholl@nist.gov

Information and Feedback
Web: csrc.nist.gov/sec-cert
Comments: sec-cert@nist.gov